

REMARKS

Claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 and 55-63 are pending in the present application, of which claims 1, 5, 9, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 60 and 62 are amended and are independent and claims 4, 8, 12, 59, 61 and 63 are amended and are dependent. Applicant believes that the present application is in condition for allowance, which prompt and favorable action is respectfully requested.

I. REJECTION UNDER 35 U.S.C. §103

The Office Action rejected claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 and 55-63 under 35 U.S.C. §103 as being unpatentable over U.S. Patent Re. 33,189 issued to Lee et al. (hereinafter "Lee") in view of U.S. Patent No. 5,870,474 by Wasilewski et al. (hereinafter "Wasilewski") and further in view of U.S. Patent No. 6,424,947 by Tsuria et al. (hereinafter "Tsuria"). In view of the amendments to independent claims 1, 5, 9, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 60 and 62, the rejection is moot.

Lee teaches a symmetric key security system in which a user ID is distributed from a user database on a billing computer 10 (SSTV Transmitter) to a subscriber receiver (SSTV Receiver) prior to installation to installation of the subscriber receiver. (See Fig. 1, Col. 3, line 65 to Col. 4 line 7). The user ID is used to encrypt a secret key on the billing computer 10 which is also sent to the subscriber receiver.

The Office has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art references must teach or suggest all the claim limitations. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one

of ordinary skill in the art, to modify the reference or to combine reference teachings. Third, there must be a reasonable expectation of success. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria.

In order to clarify the claims, independent claims 1, 5, 9, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 60 and 62, and dependent claims 4, 8, 12, 59, 61 and 63 are herein amended. Applicant submits that these amendments clarify previously inherent features and do not narrow the scope of the amended claims.

Claims 1, 22, 40, and 58

Claimed Elements are Not Taught or Suggested by the Prior Art

As to *Claims 1, 22, 40, and 58*, Applicant submits that Lee, Wasilewski, and Tsuria fail to teach “distributing, over-the-air from the terminal, a public key corresponding to the private key” and “receiving, over-the-air at the terminal, a secret key encrypted by the public key” as claimed. The Office Action relies primarily on Lee as teaching these limitations. Lee teaches that the transmitter on the billing computer 10 transmits both the user ID and the key (see Col. 3 lines 27-42) while the subscriber receiver (terminal) only receives the user ID and the key. By contrast, the claimed terminal distributes the public key and receives the secret key. Thus, Lee fails to teach these elements of the claimed method within the recited system architecture. Similarly, while Wasilewski teaches a conditional access model for content transmitted over a wired digital network using a public-private key pair, it also fails to teach the claimed sequence of distributing a public key from a terminal and receiving a secret key encrypted with the public key. Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a

localized short-range wireless link with a second smartcard reader in a remote control. However, Tsuria also fails to teach the claimed sequence of distributing a public key from a terminal and receiving a secret key encrypted with the public key.

Lee also fails to teach distribution of the public key as claimed. Lee makes it clear that the user ID is installed on the subscriber receiver prior to installation. (See Fig. 1, and Col. 3 line 65 to Col. 4 line 1). Applicant maintains that the user ID codes are set in the subscriber receiver at installation and are not "distributed" since the user ID is not obtained in the course of the terminal obtaining a secret key as claimed.

Additionally, because Lee teaches a symmetric key system, there is no "private key" corresponding to the public key. That is, the user ID described by Lee has no corresponding private key as claimed.

No Motivation to Combine Cite References

Assuming, *arguendo*, that every claimed element is taught by the prior art, Applicant further submits that there is no motivation to combine Lee, Wasilewski, and Tsuria as alleged in the Office Action.

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." *In re Linter*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972). The teaching or suggestion to make the claimed combination must be found in the prior art, not in the Applicant's disclosure.

Lee teaches a symmetric key security scheme while Wasilewski describes an asymmetric key (public-private key) security scheme. These are very distinct forms of cryptography, each aimed at different system architectures and requirements. Lee describes a symmetric key system

in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Applicant submits that there is no motivation taught in either Lee, Wasilewski, or Tsuria to combine these references and replace the symmetric key system of Lee with the asymmetric key system of Wasilewski.

Additionally, Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. Applicant submits that the problem being solved by Tsuria (i.e., localized communications between a set-top receiver and a remote control) is quite distinct from the key security scheme between a content provider and subscriber receiver being addressed in the present claims. Consequently, Applicant submits that there is no motivation to combine Tsuria with either Lee or Wasilewski.

No Reasonable Expectation of Success

Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee. In particular, the subscriber devices would now control the user ID while the billing computer 100 would have no control over such user ID. Thus, the system architecture described by Lee is inconsistent with the asymmetric key scheme described by Wasilewski. Not only is there no teaching or suggestion to replace the symmetric key scheme of Lee with the asymmetric key scheme of Wasilewski, but doing so would completely change the system architecture taught by Lee, including the interaction between the billing

computer and subscriber receivers. Consequently, Applicant submits that there is reasonable expectation of success in combining Lee, Wasilewski and Tsuria.

Therefore, Applicant respectfully submits that the Office Action has failed to set forth a prima facie case of obviousness as to claims 1, 22, 40, and 58.

Claims 5, 25, 43, and 60

Claimed Elements are Not Taught or Suggested by the Prior Art

As to *Claims 5, 25, 43, and 60*, Applicant submits that Lee, Wasilewski, and Tsuria fail to teach “distributing, over-the-air from the terminal, a public key corresponding to the private key” and “receiving, over-the-air at the terminal, the broadcast access key encrypted by the public key” as claimed. The Office Action relies primarily on Lee as teaching these limitations. Lee teaches that the transmitter on the billing computer 10 transmits both the user ID and the key (see Col. 3 lines 27-42) while the subscriber receiver (terminal) only receives the user ID and the key. By contrast, the claimed terminal distributes the public key and receives the access key. Thus, Lee fails to teach the claimed method within the recited system architecture. Similarly, while Wasilewski teaches a conditional access model for content transmitted over a wired digital network using a public-private key pair, it also fails to teach the claimed sequence of distributing a public key from a terminal and receiving a secret key encrypted with the public key. Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. However, Tsuria also fails to teach the claimed sequence of distributing a public key from a terminal and receiving an access key encrypted with the public key at the terminal .

Lee also fails to teach distribution of the public key as claimed. Lee makes it clear that the user ID is installed on the subscriber receiver prior to installation. (See Fig. 1, and Col. 3 line 65 to Col. 4 line 1). Applicant maintains that the user ID codes are set in the subscriber receiver (terminal) at installation and are not "distributed" since the user ID is not obtained in the course of the terminal obtaining an access key as claimed.

Additionally, because Lee teaches a symmetric key system, there is no "private key" corresponding to the public key. That is, the user ID described by Lee has no corresponding private key as claimed.

No Motivation to Combine Cite References

Assuming, *arguendo*, that every claimed element is taught by the prior art, Applicant further submits that there is no motivation to combine Lee, Wasilewski, and Tsuria as alleged in the Office Action.

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." *In re Linter*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972). The teaching or suggestion to make the claimed combination must be found in the prior art, not in the Applicant's disclosure.

Lee teaches a symmetric key security scheme while Wasilewski describes an asymmetric key (public-private key) security scheme. These are very distinct forms of cryptography, each aimed at different system architectures and requirements. Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee, including the

interaction between the billing computer and subscriber receivers. Applicant submits that there is no motivation taught in either Lee, Wasilewski, or Tsuria to combine these references and replace the symmetric key system of Lee with the asymmetric key system of Wasilewski.

Additionally, Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. Applicant submits that the problem being solved by Tsuria (i.e., localized communications between a set-top receiver and a remote control) is quite distinct from the key security scheme between a content provider and subscriber receiver being addressed in the present claims. Consequently, Applicant submits that there is no motivation to combine Tsuria with either Lee or Wasilewski.

No Reasonable Expectation of Success

Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee. In particular, the subscriber devices would now control the user ID while the billing computer 100 would have no control over such user ID. Thus, the system architecture described by Lee is inconsistent with the asymmetric key scheme described by Wasilewski. Not only is there no teaching or suggestion to replace the symmetric key scheme of Lee with the asymmetric key scheme of Wasilewski, but doing so would completely change the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Consequently, Applicant submits that there is reasonable expectation of success in combining Lee, Wasilewski and Tsuria.

Therefore, Applicant respectfully submits that the Office Action has failed to set forth a prima facie case of obviousness as to claims 5, 25, 43, and 60.

Claims 9, 28, 46, and 62

Claimed Elements are Not Taught or Suggested by the Prior Art

As to *Claims 9, 28, 46, and 62*, Applicant submits that Lee, Wasilewski, and Tsuria fail to teach “receiving, over-the-air at the terminal, a public key corresponding to a private key for the terminal” and “sending, over-the-air from the terminal, the encrypted secret key” as claimed. The Office Action relies primarily on Lee as teaching these limitations. Lee teaches that the transmitter on the billing computer 10 transmits both the user ID and the key (see Col. 3 lines 27-42) while the subscriber receiver (terminal) only receives the user ID and the key. By contrast, the claimed terminal receives the public key and distributes the secret key. Thus, Lee fails to teach the claimed method within the recited system architecture. Similarly, while Wasilewski teaches a conditional access model for content transmitted over a wired digital network using a public-private key pair, it also fails to teach the claimed sequence of receiving a public key at a terminal and sending a secret key encrypted with the public key from the terminal. Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. However, Tsuria also fails to teach the claimed sequence of receiving a public key at a terminal and sending a secret key encrypted with the public key from the terminal.

Lee also fails to teach receiving the public key as claimed. Lee makes it clear that the user ID is installed on the subscriber receiver (terminal) prior to installation. (See Fig. 1, and Col. 3 line 65 to Col. 4 line 1). Applicant maintains that the user ID codes of Lee are set in the subscriber receiver (terminal) at installation and are not “received” since the user ID is not obtained in the course of the terminal obtaining a secret key as claimed.

Additionally, because Lee teaches a symmetric key system, there is no "private key" corresponding to the public key. That is, the user ID described by Lee has no corresponding private key as claimed.

No Motivation to Combine Cite References

Assuming, *arguendo*, that every claimed element is taught by the prior art, Applicant further submits that there is no motivation to combine Lee, Wasilewski, and Tsuria as alleged in the Office Action.

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." *In re Linter*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972). The teaching or suggestion to make the claimed combination must be found in the prior art, not in the Applicant's disclosure.

Lee teaches a symmetric key security scheme while Wasilewski describes an asymmetric key (public-private key) security scheme. These are very distinct forms of cryptography, each aimed at different system architectures and requirements. Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Applicant submits that there is no motivation taught in either Lee, Wasilewski, or Tsuria to combine these references and replace the symmetric key system of Lee with the asymmetric key system of Wasilewski.

Additionally, Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a

remote control. Applicant submits that the problem being solved by Tsuria (i.e., localized communications between a set-top receiver and a remote control) is quite distinct from the key security scheme between a content provider and subscriber receiver being addressed in the present claims. Consequently, Applicant submits that there is no motivation to combine Tsuria with either Lee or Wasilewski.

No Reasonable Expectation of Success

Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee. In particular, the subscriber devices would now control the user ID while the billing computer 100 would have no control over such user ID. Thus, the system architecture described by Lee is inconsistent with the asymmetric key scheme described by Wasilewski. Not only is there no teaching or suggestion to replace the symmetric key scheme of Lee with the asymmetric key scheme of Wasilewski, but doing so would completely change the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Consequently, Applicant submits that there is reasonable expectation of success in combining Lee, Wasilewski and Tsuria.

Therefore, Applicant respectfully submits that the Office Action has failed to set forth a prima facie case of obviousness as to claims 9, 28, 46, and 62.

Claims 13, 31 and 49

Claimed Elements are Not Taught or Suggested by the Prior Art

As to *Claims 13, 31 and 49*, Applicant submits that Lee, Wasilewski, and Tsuria fail to teach "receiving, over-the-air at the content provider, a public key corresponding to a private

key” and “sending, over-the-air from the content provider, the encrypted secret key” as claimed.

The Office Action relies primarily on Lee as teaching these limitations. Lee teaches that the transmitter on the billing computer 10 (content provider) transmits both the user ID and the key (see Col. 3 lines 27-42) while the subscriber receiver (terminal) only receives the user ID and the key. By contrast, the claimed content provider receives the public key and distributes the secret key. Thus, Lee fails to teach the claimed method within the recited system architecture.

Similarly, while Wasilewski teaches a conditional access model for content transmitted over a wired digital network using a public-private key pair, it also fails to teach the claimed sequence of receiving a public key at a content provider and sending a secret key encrypted with the public key from the content provider. Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. However, Tsuria also fails to teach the claimed sequence of receiving a public key at a content provider and sending a secret key encrypted with the public key from the content provider.

Lee also fails to teach receiving the public key as claimed. Lee makes it clear that the user ID is installed at the content provider prior to installation. (See Fig. 1, and Col. 3 line 65 to Col. 4 line 1). Applicant maintains that the user ID codes of Lee are set in the content provider at installation and are not “received” since the user ID is not obtained in the course of the content provider sending the secret key as claimed.

Additionally, because Lee teaches a symmetric key system, there is no “private key” corresponding to the public key. That is, the user ID described by Lee has no corresponding private key as claimed.

No Motivation to Combine Cite References

Assuming, *arguendo*, that every claimed element is taught by the prior art, Applicant further submits that there is no motivation to combine Lee, Wasilewski, and Tsuria as alleged in the Office Action.

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." *In re Linter*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972). The teaching or suggestion to make the claimed combination must be found in the prior art, not in the Applicant's disclosure.

Lee teaches a symmetric key security scheme while Wasilewski describes an asymmetric key (public-private key) security scheme. These are very distinct forms of cryptography, each aimed at different system architectures and requirements. Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Applicant submits that there is no motivation taught in either Lee, Wasilewski, or Tsuria to combine these references and replace the symmetric key system of Lee with the asymmetric key system of Wasilewski.

Additionally, Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. Applicant submits that the problem being solved by Tsuria (i.e., localized communications between a set-top receiver and a remote control) is quite distinct from the key security scheme between a content provider and subscriber receiver being addressed in the

present claims. Consequently, Applicant submits that there is no motivation to combine Tsuria with either Lee or Wasilewski.

No Reasonable Expectation of Success

Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee. In particular, the subscriber devices would now control the user ID while the billing computer 100 would have no control over such user ID. Thus, the system architecture described by Lee is inconsistent with the asymmetric key scheme described by Wasilewski. Not only is there no teaching or suggestion to replace the symmetric key scheme of Lee with the asymmetric key scheme of Wasilewski, but doing so would completely change the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Consequently, Applicant submits that there is reasonable expectation of success in combining Lee, Wasilewski and Tsuria.

Therefore, Applicant respectfully submits that the Office Action has failed to set forth a prima facie case of obviousness as to claims 13, 31, and 49.

Claims 16, 34 and 52

Claimed Elements are Not Taught or Suggested by the Prior Art

As to *Claims 16, 34 and 52*, Applicant submits that Lee, Wasilewski, and Tsuria fail to teach “receiving, over-the-air at the content provider, a public key corresponding to a private key” and “sending, over-the-air from the content provider, the encrypted broadcast access key” as claimed. The Office Action relies primarily on Lee as teaching these limitations. Lee teaches that the transmitter on the billing computer 10 (content provider) transmits both the user ID and

the key (see Col. 3 lines 27-42) while the subscriber receiver (terminal) only receives the user ID and the key. By contrast, the claimed content provider receives the public key and sends the access key. Thus, Lee fails to teach the claimed method within the recited system architecture. Similarly, while Wasilewski teaches a conditional access model for content transmitted over a wired digital network using a public-private key pair, it also fails to teach the claimed sequence of receiving a public key at a content provider and sending an access key encrypted with the public key from the content provider. Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. However, Tsuria also fails to teach the claimed sequence of receiving a public key at a content provider and sending an access key encrypted with the public key from the content provider.

Lee also fails to teach receiving the public key as claimed. Lee makes it clear that the user ID is installed at the content provider prior to installation. (See Fig. 1, and Col. 3 line 65 to Col. 4 line 1). Applicant maintains that the user ID codes of Lee are set in the content provider at installation and are not “received” since the user ID is not obtained in the course of the content provider sending an access key as claimed.

Additionally, because Lee teaches a symmetric key system, there is no “private key” corresponding to the public key. That is, the user ID described by Lee has no corresponding private key as claimed.

No Motivation to Combine Cite References

Assuming, *arguendo*, that every claimed element is taught by the prior art, Applicant further submits that there is no motivation to combine Lee, Wasilewski, and Tsuria as alleged in the Office Action.

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." *In re Linter*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972). The teaching or suggestion to make the claimed combination must be found in the prior art, not in the Applicant's disclosure.

Lee teaches a symmetric key security scheme while Wasilewski describes an asymmetric key (public-private key) security scheme. These are very distinct forms of cryptography, each aimed at different system architectures and requirements. Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Applicant submits that there is no motivation taught in either Lee, Wasilewski, or Tsuria to combine these references and replace the symmetric key system of Lee with the asymmetric key system of Wasilewski.

Additionally, Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. Applicant submits that the problem being solved by Tsuria (i.e., localized communications between a set-top receiver and a remote control) is quite distinct from the key security scheme between a content provider and subscriber receiver being addressed in the present claims. Consequently, Applicant submits that there is no motivation to combine Tsuria with either Lee or Wasilewski.

No Reasonable Expectation of Success

Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee. In particular, the subscriber devices would now control the user ID while the billing computer 100 would have no control over such user ID. Thus, the system architecture described by Lee is inconsistent with the asymmetric key scheme described by Wasilewski. Not only is there no teaching or suggestion to replace the symmetric key scheme of Lee with the asymmetric key scheme of Wasilewski, but doing so would completely change the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Consequently, Applicant submits that there is reasonable expectation of success in combining Lee, Wasilewski and Tsuria.

Therefore, Applicant respectfully submits that the Office Action has failed to set forth a prima facie case of obviousness as to claims 16, 34, and 52.

Claims 19, 37 and 55

Claimed Elements are Not Taught or Suggested by the Prior Art

As to *Claims 19, 37 and 55*, Applicant submits that Lee, Wasilewski, and Tsuria fail to teach “distributing, over-the-air from the content provider, a public key corresponding to the private key” and “receiving, over-the-air at the content provider, a secret key encrypted by the public key” as claimed. The Office Action relies primarily on Lee as teaching these limitations. Lee teaches that the transmitter on the billing computer 10 (content provider) transmits both the user ID and the key (see Col. 3 lines 27-42) while the subscriber receiver (terminal) only receives the user ID and the key. By contrast, the claimed content provider distributes the public key and

receives the secret key. Thus, Lee fails to teach the claimed method within the recited system architecture. Similarly, while Wasilewski teaches a conditional access model for content transmitted over a wired digital network using a public-private key pair, it also fails to teach the claimed sequence of distributing a public key from a content provider and receiving a secret key encrypted with the public key at the content provider. Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. However, Tsuria also fails to teach the claimed sequence of distributing a public key from a content provider and receiving a secret key encrypted with the public key at the content provider.

Lee also fails to teach distribute the public key as claimed. Lee makes it clear that the user ID is installed at the subscriber receiver prior to installation. (See Fig. 1, and Col. 3 line 65 to Col. 4 line 1). Applicant maintains that the user ID codes are set in the subscriber receiver at installation and are not “distributed” by the content provider since the user ID is not obtained in the course of the terminal obtaining a secret key as claimed.

Additionally, because Lee teaches a symmetric key system, there is no “private key” corresponding to the public key. That is, the user ID described by Lee has no corresponding private key as claimed.

No Motivation to Combine Cite References

Assuming, *arguendo*, that every claimed element is taught by the prior art, Applicant further submits that there is no motivation to combine Lee, Wasilewski, and Tsuria as alleged in the Office Action.

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the

proposed substitution, combination, or other modification." *In re Linter*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972). The teaching or suggestion to make the claimed combination must be found in the prior art, not in the Applicant's disclosure.

Lee teaches a symmetric key security scheme while Wasilewski describes an asymmetric key (public-private key) security scheme. These are very distinct forms of cryptography, each aimed at different system architectures and requirements. Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Applicant submits that there is no motivation taught in either Lee, Wasilewski, or Tsuria to combine these references and replace the symmetric key system of Lee with the asymmetric key system of Wasilewski.

Additionally, Tsuria teaches a set-top receiver having a first smartcard reader that communicates via a localized short-range wireless link with a second smartcard reader in a remote control. Applicant submits that the problem being solved by Tsuria (i.e., localized communications between a set-top receiver and a remote control) is quite distinct from the key security scheme between a content provider and subscriber receiver being addressed in the present claims. Consequently, Applicant submits that there is no motivation to combine Tsuria with either Lee or Wasilewski.

No Reasonable Expectation of Success

Lee describes a symmetric key system in which a centralized billing computer 10 controls the user ID installed in each subscriber receiver. Replacing such symmetric key scheme with an asymmetric key (public-private key) scheme would entail completely replacing the system architecture taught by Lee. In particular, the subscriber devices would now control the user ID

while the billing computer 100 would have no control over such user ID. Thus, the system architecture described by Lee is inconsistent with the asymmetric key scheme described by Wasilewski. Not only is there no teaching or suggestion to replace the symmetric key scheme of Lee with the asymmetric key scheme of Wasilewski, but doing so would completely change the system architecture taught by Lee, including the interaction between the billing computer and subscriber receivers. Consequently, Applicant submits that there is reasonable expectation of success in combining Lee, Wasilewski and Tsuria.

Therefore, Applicant respectfully submits that the Office Action has failed to set forth a prima facie case of obviousness as to claims 19, 37, and 55.

Also, claims 2-4, 8, 10-12, 14-15, 20-21 23-24, 29-30, 32-33, 38-39, 41-42, 47-48, 50-51, 56-57, 59, 61, and 63 depend from and include all the elements cited in the independent claims 1, 5, 9, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 60 and 62, respectively. Therefore, Applicant submits that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

For at least the foregoing reasons, Applicant respectfully requests a withdrawal of the rejection under 35 U.S.C. §103.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Applicant requests a two month extension of time in which to respond to the Office Action dated November 14, 2006. Please charge the requisite extension fee to Deposit Account No. 17-0026. Please charge any other fees associated with this paper to deposit Account No. 17-0026.

Respectfully submitted,

Dated: March 16, 2007

By: 

David J. Huffaker, Reg. No. 56,771
Attorney for Applicant
Telephone: 858-845-2110

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502